Transparency and Broadband ISPs

Gerald R. Faulhaber*

Introduction

Broadband Internet Service Providers (ISPs) have been front and center in the debate about a national broadband plan. While Verizon, AT&T, Comcast, Time Warner and a host of other cable firms and telephone companies (telcos) have deployed a broadband distribution network that passes an estimated 92% of American homes, many policy advocates claim that there are problems; they claim that broadband ISPs are manipulating Internet traffic to their customers for crass commercial gain, blocking access to websites that offer competing services, or otherwise managing their networks, in violation of the principle of "network neutrality." And even if we have little evidence of this at this time, the advocates assert that ISPs probably will undertake aggressive anticompetitive actions in the future. Further, advocates point to limited competition in the broadband ISP market that suggests the exercise of market power that can harm customers and the Internet itself. Lack of evidence of widespread bad behavior by broadband ISPs has not dampened advocates' enthusiasm for regulation.

Whatever the state of competition is in the broadband ISP market, and whether or not one agrees that a "network neutrality" principles or rules should govern the Internet, all parties can agree that broadband ISPs (as with any other producer of goods and services) should disclose information concerning their offerings to their customers. Broadband ISPs should be *transparent* in their dealings with customers.

Economists have long recognized that markets can only work well if both producers and consumers are well-informed about the terms and conditions of transactions; if customers don't know what they are buying, they can hardly be expected to make good purchasing decisions, and markets not only may work poorly, they may not work at all![1] Information asymmetry, when one transacting party has superior information to the counterparty, is a well-known market failure, and public policy intervention to either provide such information or mandate its provision is well accepted.[2]

---

* Professor Emeritus, Business and Public Policy Dept., Wharton School, University of Pennsylvania, and Penn Law School. The author would like to thank Jonathon Levy and John Norton, FCC; Christopher Yoo, Law School of the University of Pennsylvania; Andrea Matwyshyn, Wharton School of the University of Pennsylvania; and Joe Waz and Jason Livingood, Comcast Corporation for their valuable assistance. The opinions expressed are the author's only, who is responsible for any errors or omissions. Please direct correspondence to faulhaber@wharton.upenn.edu .

[1] The seminal paper in the importance of information for markets is Akerlof, G., THE MARKET FOR "LEMONS": QUALITY UNCERTAINTY AND THE MARKET MECHANISM, *Quarterly Journal of Economics*, 84(3), Aug 1970, 488-500.

[2] Although it is usual to assume that sellers/producers have superior information to buyers/customers, this is not necessarily the case. For example, a buyer of life insurance may have superior information to

In fact, the US economy is rife with disclosure regulations in many markets. Institutions that issue financial instruments such as stocks and bonds are subject to stringent regulations regarding disclosure of relevant information to financial markets and strict limits on "insider" trading of private information. The pharmaceutical industry faces stringent disclosure requirements for both prescription and over-the-counter medications of dosage, ingredients, and measured side effects. In the case of prescription medications, there is actually a two-level disclosure protocol: the main side effects and contraindications are listed on the label of the medication, while the complete list of clinical results is disclosed in a package insert. The packaged food industry is required by the FTC and FDA to include on the package label a standardized information panel of nutrition data; an example is duplicated below to remind the reader of how ubiquitous these labels are.

Nutrition Facts

Serving Size 29 g

Amount Per Serving			
Calories 94		Calories from Fat 57	
		% Daily Value*	
Total Fat 6g			10%
Saturated Fat 2g			8%
Trans Fat			
Cholesterol 23mg			8%
Sodium 93mg			4%
Total Carbohydrate 3g			1%
Dietary Fiber 0g			0%
Sugars			
Protein 6g			
Vitamin A	1% •	Vitamin C	0%
Calcium	1% •	Iron	2%

*Percent Daily Values are based on a 2,000 calorie diet. Your daily values may be higher or lower depending on your calorie needs.

NutritionData.com

Figure 1 Example Nutritional Label from Packaged Food

Disclosure is of particular value in markets with information asymmetries, where producers possess information that customers do not have, and can not be easily discerned from inspecting the product or service pre-transaction. Firms may choose to disclose some or all of the information relevant to customers' buying decisions, or government regulations may require disclosure (as in the examples above).[3] Even if firms choose to disclose information, the disclosure may not be truthful; the FTC, for

the seller of a pre-existing medical condition that affects the buyer's likely expected lifetime and may strategically withhold such information when executing a life insurance transaction.

[3] Disclosure is not the only way that decision-relevant information reaches customers. Customers often learn post-transaction about products, and firms gain reputations for their quality and service. In fact, various information intermediaries such as newspapers, magazines and websites may offer reviews of products to help inform customers.

example, has long imposed truth-in-packaging regulations to ensure that voluntary disclosures are indeed truthful and therefore informative.[4]

Disclosure and Broadband

Broadband ISP is a service which is likely to suffer from information asymmetries. Customers are offered a service which provides data speeds "up to" 12 Mbps, which may be subject to network management during peak periods without notification, which may or may not offer effective protections against spam, viruses and worms, and which may selectively block/delay some applications without notification. Can customers make good purchasing decisions without more complete information?

The question answers itself; broadband distribution is a complex service with several dimensions that are important to customers, about which only the producer can supply the relevant information. Further, it is not sufficient to argue that competition among providers will solve the problem of information asymmetry; the classic paper by Akerlof *op. cit.* (fn 1) shows that information asymmetries can cause the collapse of a market even if competitive.[5]

However, it would be a grievous error to confine our transparency focus only to broadband ISPs. Very serious disclosure problems exist with application providers (websites and other Internet applications). Internet customers are under significant threat from compromised websites and other applications that may leave worms on their computers, steal financial information, and even turn their computers into zombie bots. Yet there appear to be few existing disclosure requirements (other than obscure and difficult to find privacy policies) on application providers.

A particularly egregious example involves the election campaign of Norm Coleman, contesting an election for the US Senate in Minnesota, that sent potential supporters an e-mail, providing a link

> "...to read more about the candidate and donate online. On the day the campaign sent the email, it knew the website was under attack and

---

[4] Firms that sell high quality goods and services will often use disclosure as a means of distinguishing their products from firms that sell lower quality goods and services; a requirement for truthful disclosure makes such a strategy feasible, as firms producing poor quality cannot claim otherwise and so high quality firms can credibly signal to customers that they are indeed high quality.

[5] The FCC recognized this in its recent Comcast Order: "Although Comcast and certain other commenters contend that competition among broadband Internet access providers is sufficient to address any concerns regarding network management practices, they do not address the effects of this information asymmetry between the broadband Internet access provider and its customers and competitors." Federal Communications Commission, FORMAL COMPLAINT OF FREE PRESS AND PUBLIC KNOWLEDGE AGAINST COMCAST CORPORATION FOR SECRETLY DEGRADING PEER-TO-PEER APPLICATIONS, Memorandum Opinion and Order, August 20, 2008, FCC 08-183, fn 242, p. 32.

> compromised. Because consumers visited the campaign website and donated, their credit card data may have been stolen…"[6]

In fact, the *security breach was known by the campaign in January, 2009, and not disclosed by the campaign until March 11, 2009*, after the breach was exposed by third parties.[7]

Other application providers can cause mischief with customers, even users of the Internet that are not direct customers. The well-known P2P file sharing application BitTorrent[8] was released in 2001 by programmer Bram Cohen. The application uses a protocol of Cohen's design that increases download/upload speeds dramatically using methods that can significantly decrease the speeds available to other Internet broadband customers not using BitTorrent.[9] Far from being an unintended consequence of the protocol design, this feature was designed in at the outset:[10]

> "Peer-to-peer users of BitTorrent are a bandwidth-hungry minority … Cohen [inventor of BitTorrent] says … he predicted [this] when he first thought up BitTorrent."My whole idea was, 'Let's use up a lot of bandwidth,'" he laughs. "I had a friend who said, 'Well, ISPs won't like that.' And I said, 'Why should I care?'""

Clearly, the practices of application providers are as much in need of full disclosure/transparency as those of broadband ISPs. Although the focus of this paper is transparency of broadband ISPs (to which we now return), we cannot lose sight of the fact that customers' need for transparency in the broadband Internet[11] extends well beyond the broadband ISP market.

In some circumstances, we may count on market forces to result in voluntary disclosure of relevant information, but such circumstances do not appear to be present in the broadband ISP market (nor in the application provider market, as the above examples illustrate). In a recent unfortunate incident, Comcast chose to block/delay certain upstream traffic using the P2P BitTorrent protocol for network management reasons,

---

[6] Matwyshyn, A., HIDDEN ENGINES OF DESTRUCTION, forthcoming, *Florida Law Review*, 2010, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=958437 .

[7] Mills, E., COLEMAN SENATE CAMPAIGN IN DONOR DATA LEAK MESS, *CNET News*, March 12, 2009

[8] See Wikipedia (2009), BitTorrent (protocol) at http://en.wikipedia.org/wiki/BitTorrent_(protocol) .

[9] "The web response time statistic increased from a value of 0.25 seconds when no BitTorrent users were active to 0.65seconds when 15 BitTorrent users were active. This suggests that 15 BitTorrent users can cause a drop in performance by a factor of 2.5." From Martin, J. and Westall, J., ASSESSING THE IMPACT OF BITTORRENT ON DOCSIS NETWORKS, in *Proceedings of the Fourth International Conference on Broadband Communications, Networks and Systems*, Sept 14, 2007, pp. 423-432.

[10] Downs, D., BITTORRENT, COMCAST, EFF ANTIPATHETIC TO FCC REGULATION OF P2P TRAFFIC, *SFWeekly*, January 22, 2008, at http://www.sfweekly.com/2008-01-23/news/bittorrent-comcast-eff-antipathetic-to-fcc-regulation-of-p2p-traffic/print

[11] See, for example, Faulhaber, G., A NATIONAL BROADBAND PLAN FOR OUR FUTURE: A CUSTOMER-CENTRIC APPROACH, *International Journal of Communication* 3, 2009, pp. 742-779 at http://ijoc.org .

but did not disclose this practice to its customers (or indeed anyone). After several third parties conducted tests which showed that Comcast was involved in throttling BitTorrent, the FCC investigated a complaint and ordered Comcast to change its network management practices (see Federal Communications Commission, *op. cit.*). But most interesting for the purposes of this paper was the FCC's finding that Comcast had not disclosed its practices to its customers, and obfuscated about its practices when confronted with test data from third parties verifying its throttling. Apparently, the lack of transparency was as objectionable to the FCC as was the underlying action of traffic throttling.[12] So it would appear that we cannot expect voluntary disclosure of all relevant information by broadband ISPs to their customers.

If mandate disclosure we must, then *what* should be disclosed, *why* should it be disclosed, *when* and *where* should it be disclosed, and perhaps most important *how* should it be disclosed? The next sections of this paper address these questions, first by establishing general principles that govern disclosure in *any* industry, which I illustrate with examples from multiple US industries and agencies. Second, I review the disclosure practices currently mandated or otherwise in place, both in the US and selected overseas jurisdictions. Third, I review the special disclosure challenges in the broadband ISP industry that the FCC (or any agency) must face.

The point of this paper is not to suggest or recommend who should disclose what and when. It is rather to outline when mandated disclosure is required, what are the guiding principles for successful disclosure policies, what has been the current experience in this industry, and what are the challenges policymakers must overcome in this industry for transparency to do its work.

Disclosure in General – Four Principles

Mandated disclosure/transparency is well-established in many sectors of our economy, so it is possible to derive a number of principles for successful disclosure rules. In this section, I suggest four principles, illustrating each using examples from other industries.

The *first* principle is the touchstone from which all others follow: **disclose all information** (and only such information) **that a reasonable customer needs to make an informed purchase decision.** The focus is on the customer when determining the structure and content of disclosure.

A principal activity in which disclosure has a long and rich history is securities regulation, particularly the obligation of corporations to disclose "material" information

[12] In previous work, I argue that Comcast could have avoided this unfortunate incident using good disclosure practices. See Faulhaber, G. "NETWORK NEUTRALITY: THEORY AND PRACTISE," Chapter 17 in Madden G., ed., *The Economics of Digital Markets*, Edward Elgar, Cheltenham: 2009.

to shareowners and the market in a timely fashion. For example, information is material for purposes of creating the basis of an insider trading action if "there is a substantial likelihood that a reasonable shareholder would consider it important" in deciding how to act. See TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976).[13] This established the "reasonable shareholder" standard for materiality of information, and one that can usefully be employed in other contexts, including broadband ISP disclosure (substituting "reasonable customer").

The FCC itself recognized this standard (although not by explicit reference) in its Comcast Order[14]:

> "...disclosure of ... practices to consumers in a manner that customers of ordinary intelligence would reasonably understand would enhance the "vibrant and competitive free market . . . for the Internet and interactive computer services" by allowing consumers to compare and contrast competing providers' practices."

And

> "[D]isclosed information must provide enough detail to enable customers to make an informed decision and to enable them to adjust their behavior."[15]

These examples highlight the focus on the customer, and establish a standard of disclosure of information that a "reasonable customer" would find material in his/her purchasing decision.

So who should be the judge of what information the "reasonable customer" needs? While there will no doubt be many self-styled experts and consumer advocates willing to "represent" the reasonable customer, I would suggest that primary reliance when determining disclosure regulations should be on what customers themselves think they need to know, and in what form. Focus groups of actual customers are more likely to be a reliable source of information than the advice of these self-styled experts and consumer advocates.

In the context of informed consent for digital products (such as DRM-protected media), Matwyshyn proposes a "reasonable digital consumer" standard for informed consent established using real-world consumers (drawing on trademark law):

---

[13] Quoted in Matwyshyn, A. MATERIAL VULNERABILITIES: DATA PRIVACY, CORPORATE INFORMATION SECURITY AND SECURITIES REGULATION, *Berkeley Business Law Journal, Vol. 3, p. 129, 2005.*
[14] See Federal Communications Commission, *op. cit.*, ¶ 52, p. 32.
[15] *Ibid*, fn 240, p. 32, quoting testimony by van Schewick.

> "...creat[e] an objective "reasonable digital consumer" standard based on empirical testing of real consumers. In a manner similar to the way in which courts empirically assess actual consumer confusion in trademark law, the primary vehicle of digital consent, digital user agreements, can be tested for legal usability."[16]

The first principle, then, (i) focuses on disclosure of information that the customer needs to make an informed purchase decision, (ii) uses a "reasonable customer" standard, similar to the reasonable investor standard in securities law and the reasonable consumer standard in consumer law, and (iii) relies on actual customers rather than experts or advocates to determine what information they need.

The *second* principle is **easy access** to the disclosed information. Customers need to have the information at the point of purchase or use; forcing customers to dig through bill inserts, interminable and incomprehensible privacy statements, or multiple web pages is not acceptable and does not constitute disclosure.

Perhaps the best model of accessibility is the Nutrition Data panel on all packaged foods shown in Figure 1.[17] It is literally on the package itself; the information is disclosed directly to the customer while in the act of consumption/purchase. While the customer is not actually required to read the label, there is no need to search for the information or consult other material. It is right there, and it has the nutritional information the customer needs.

A second example is disclosure of medical indications of prescription and OTC medications in the US. Medications are generally very complex products with a number of possible side-effects and drug interactions, all of which are important to the customers. Drug labeling must strike a balance between easy access and completeness.[18] The solution is to list the main side effects on the drug container itself, highly visible at the point of purchase/consumption, and then to have a more complete list of all know medical indications on a package insert. While customers are likely to

---

[16] Matwyshyn, A. TECHNOCONSEN(T)SUS, *Washington University Law Review*, **85**(529), 2007 at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=904075 .

[17] For more information on consumer product labeling, see Federal Trade Commission (2008). FTC BASIC LABELING REQUIREMENTS FOR CONSUMER PACKAGES, at www.science.oas.org/SIM/organization/twg/SurveyUSA.doc

[18] For more information on prescription drug labeling, see Food and Drug Administration (2008) Center for Drug Evaluation and Research, INTRODUCTION TO THE IMPROVED FDA PRESCRIPTION DRUG LABELING, *Center for Drug Evaluation and Research* at http://www.fda.gov/Training/ForHealthProfessionals/ucm090590.htm.

read the most important side effects on the container, the inclusion of the package insert makes available full information as part of the customer actually handling the product.

It is also worth noting that both print and television advertisements for prescription medications are required to disclose in the ad itself major side effects and limitations of the medication. This ensures that customers have the information they need not only at the point of purchase/consumption, but at the time an invitation to purchase is extended.

Not all disclosure practices provide such easy access. Privacy policies on websites that require multiple click-throughs for the customer to finally find a densely worded text are the antithesis of easy access.

The *third* principle is **clarity and simplicity** of disclosed information. Again, the Nutrition Data panel is an illustration of this principle, for several reasons:

1. The panel contains only 14 numbers, clearly labeled. Reasonably knowledgeable customers are aware of the importance of each number: calories, fat, protein, etc. The panel does not offer advice, lecture the customer, or otherwise depart from a pure data format. It offers both absolute levels of nutritional elements as well as their percentage of Daily Value (which is briefly described in the panel.
2. Other numbers may be useful or relevant to some subset of customers, but are not included to avoid information overload. For example, glycemic load is an important nutritional element for diabetics but is not included in the standard panel in the interest of simplicity.
3. The panel is absolutely uniform in content, format and presentation. The Nutrition Data panel on salad dressing is identical to the panel on frozen food or candy. Customers can easily assimilate information in a format which they have seen hundreds of times. They need not spend effort figuring out what the panel format is for, say, Wishbone salad dressing, because it is the same format for every packaged food. Standardization of format facilitates side-by-side customer comparison shopping, and thus aids in purchasing decisions.

Similarly, with more complex products such as prescription medications, simplicity and clarity are important. As noted above, customer-relevant information of greatest importance to most customers is clearly and simply stated directly on the package label, and customers are accustomed to being able to access it directly. More detailed and complete information is contained in a package insert, which is necessarily more complex.

Another example of clear and simple disclosure standards is that of financial reporting for publicly traded companies. Firms are required to report, to their shareowners and the investing public, their income statement and balance sheet in their annual report. The income statement and balance sheet (IS/BS) are a standard format established by the Financial Accounting Standards Board, used by all auditing firms and reporting corporations. The IS/BS contains the most important information concerning a firm's financial position: revenues from various sources, operating costs of various forms, assets and liabilities. There is more detail available, and reported quarterly, in the firm's 10-K report, filed with the SEC. Again, a key to effective disclosure is that the IS/BS is (relatively) simple and clear, and produced in a standard format across the economy. This permits the IS/BS to be used by investors in their purchase and sale decisions regarding firms, without great effort to disentangle the meaning of the report.

In contrast, application firms both on an off the Internet sell their products along with an End User License Agreement (EULA), usually requiring customers to agree fully with all terms in the EULA. Traditionally, EULAs are quite long and appear to have been written with obfuscation in mind. They are neither clear nor simple; it is perhaps not surprising that they strip customers of most of their rights to redress under product liability.

Privacy policies, required of both broadband ISPs and application providers who handle personally identifiable information of customer, are a mixed bag. Privacy policies are always at least one click away from what a customer usually sees, and often hidden several levels down. In many cases, written privacy policies are confusing and unclear, and certainly not simple. Firms that are likely to earn significant returns from the sale/sharing of customer information are also likely to use a kerfuffle of legalese to obscure their actual practices, which they are required to disclose. Others are clearer and more open about privacy practice disclosure, but this is an area in which disclosure could be much improved.

The *fourth* principle is **verifiability**. If a firm discloses relevant information in an easily accessible, clear and simple format, but the information is false or misleading, then this is worse for customers than no information at all. Consumer products claiming "new and improved" or "organic" have little credibility with customers unless such labeling passes muster with the relevant government agency such as the FTC. Firms that claim "earnings up 35%" have little credibility unless the claim is supported by an independent auditor and the supporting IS/BS filed with the Securities and Exchange Commission. Auto firms claiming their cars are the most reliable have little credibility with customers unless the claim is supported by a ratings firm such as J.D. Powers.

There are various routes to verifiability, each of which may have their place in the broadband ISP industry.

1. Process standards-based. A standard of performance is adopted and the firm is audited against that standard, which it may advertise or be required to disclose. The ISO 9000 family of industrial standards functions in this fashion. The firm retains an auditor that examines the processes and practices of the firm and certifies if they are in compliance.
2. Results audit. A performance measure, such as mean-time-to-failure or level of customer satisfaction, is audited on a regular basis by an outside auditor which

then reports the results, often making them public. The performance measure is usually an industry-standard measure, possibly determined by an engineering body or management practices organization, which is common across all firms.

3. Regulatory audit. A series of performance measures, likely defined by an engineering body or a management practices organization, determined to be the relevant measures for the regulated firm, are evaluated by the firm according to established and auditable procedures or by an outside auditor or (less often) the regulatory body. Results are reported on a regular basis and made public.

Disclosure of the results of the audit may be mandated on the firm, or the results may be made public by the regulatory (or other) body in a format convenient for customers to compare performance of all audited firms side-by-side.

Disclosure of packaged food nutritional data and prescription medication data derives from information generated by each firm using standard processes and subject to review and certification by the FDA. FDA-related mandated disclosure would be an illustration of #3, above. Disclosure of the financial information of publicly traded firms is always accompanied by the name of the accounting firm that performed the audit as well as their attestation of its accuracy. SEC-mandated disclosure would be an example of #2, above.

Broadband Disclosure Today – Current Practices

Broadband Internet service is a rather new industry which the FCC has considered an 'information service', subject to little or no regulation. There appears to have been no disclosure requirements for broadband ISPs until very recently. Even for cable television service, the disclosure requirements imposed by the FCC relate only to what must[19] or may[20] appear on the customer's bill, as well as minimal customer service requirements[21]. Beyond that, further disclosure is left to local jurisdictions.

The Federal Trade Commission is the most likely agency to formulate and enforce mandated disclosure regulation, as it is the lead Federal agency for consumer protection issues.[22] Indeed, the FTC's Staff Report on broadband competition[23] noted:

> "Internet access implicates two broad areas of consumer protection: (1) clear and conspicuous disclosure of material terms of Internet access services; and (2) security and privacy issues created by broadband Internet access services."

---

[19] 47 CFR 76.952

[20] 47 CFR 47 CFR 76.985

[21] 47 CFR 76.1602-3 and 76.309

[22] Of course, the FCC has a leadership role in consumer protection for telecommunications customers.

[23] Staff Report, BROADBAND CONNECTIVITY COMPETITION POLICY, *Federal Trade Commission*, June 2007, at http://www.ftc.gov/reports/broadband/v070000report.pdf , p. 9.

Surprisingly, the Staff Report has no specific recommendations about disclosure, other than a general dictum to "continue to enforce the consumer protection laws in the area of broadband Internet access."[24,25] Then-Chairperson Deborah Platt Majoras spoke strongly[26] about disclosure in the online world:

> "technology evolves, but general FTC standards for disclosures remain constant – 'clear and conspicuous disclosure of material terms' prior to purchase."

This language is quite similar to the four principles put forth above. Unfortunately, there appears to be scant reflection of this principle in the broadband ISP market.

The FTC, however, has been quite active in pressing websites to adopt privacy statements and in enforcing such statements. In a report to Congress in 2000,[27] the FTC assessed the "self-regulation" approach then (and now) in place. A study was commissioned by an outside academic, reviewing the privacy policies of selected websites. These policies were evaluated using the FTC's "widely accepted fair information practices" of Notice, Choice, Access and Security,[28] and found that the results of self-regulation fell far short of acceptable and non-deceptive privacy disclosure. The Commission recommended legislation to Congress for a mandatory privacy statement law. Congress did not act at that time, and self-regulation of website privacy statements continues to be the norm. After 2000, there were no more reports to Congress on privacy issues.

The FTC continues its interest in this area. Lack of mandated privacy disclosure limits FTC enforcement activities to bringing cases against firms whose websites contain a privacy policy that they are violating. Nevertheless, the FTC is active in this area.[29] The statutory authority for FTC action in such cases is Section 5 of the Federal Trade Commission Act,[30] which forbids unfair or deceptive acts or practices. However, if a firm has no privacy policy, the FTC has no basis for action.[31]

---

[24] *Ibid.*, p. 162

[25] Inquiries at the FTC for further information were not successful at the time of this writing.

[26] Majoras, D., THE FTC: WORKING TO PROTECT CONSUMERS IN THE ON-LINE WORLD, *presented at the Federal Communications Bar Association*, June 27, 2007 at http://www.ftc.gov/speeches/majoras/070627fcba.pdf.

[27] PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE – A REPORT TO CONGRESS, *Federal Trade Commission*, May, 2000, at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[28] *Ibid.* p. iii. A fifth principle of Enforcement is sometimes added. Note the similarity of these principles to those espoused in this paper.

[29] UNFAIRNESS & DECEPTION: ENFORCING PRIVACY PROMISES: SECTION 5 OF THE FTC ACT, *Federal Trade Commission*, at http://www.ftc.gov/privacy/privacyinitiatives/promises.html.

[30] U.S.C. §§ 41-58, as amended.

[31] A recent article suggests that websites be required to prominently display the equivalent of a Nutrition Label which explains how the website complies with each of the Fair Information Practices. See Ciochetti,

As a result of the Comcast Order (FCC, *op. cit.*), Comcast's disclosure practices have changed substantially. In Comcast's letter to the FCC,[32] Comcast describes in detail how they will inform customers about the transition to their new network management practices. These practices include publication of Comcast's Acceptable Use Policy as updated; posting of information concerning the design and trial of Comcast's new network management to their Network Management Policy webpage; posting new Frequently Asked Questions explaining the new AUP and network management practices; and sending e-mails to all customers two weeks prior to the commercial deployment of the new practices.

Since the Order, Comcast appears to have significantly beefed up its customer disclosure, primarily via their website. This includes statements of their Subscriber Agreement,[33] Acceptable Use Policy,[34] Network Management Policy,[35] Privacy Policy,[36] and Security.[37] Links to these web pages are provided at the bottom of the Comcast.net opening web page (www.comcast.net). In addition, Comcast claims to use e-mail to disseminate important information to its customers.

It would appear that Comcast has taken the transparency critique seriously. This event also appears to have impacted other broadband ISPs; checking the websites of both Verizon and AT&T reveals similar disclosure policies.

While this extensive level of disclosure by broadband ISPs is to be welcomed, it is useful to analyze this disclosure using the principles above:

1. Does this disclosure provide all the information a customer would need to make an informed purchase decision?
2. Does the customer have "easy access" to the disclosed information?
3. Is the disclosed information "clear and simple"?
4. Is the disclosed information "verifiable"?

It is not the purpose of this paper to critique Comcast's or any other firm's disclosure policy; the reader is invited to apply the principles of this paper to this and other

C., THE FUTURE OF PRIVACY POLICIES: A PRIVACY NUTRITION LABEL FILLED WITH FAIR INFORMATION PRACTICES, *John Marshall Journal of Computer Law and Information*, **26**(1) pp. 1-45, 2009.

[32] Letter from Comcast to FCC at http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6520169715 ("Comcast Compliance Plan"), Attachment C, p. 2.

[33] See http://www.comcast.net/terms/subscriber/ .

[34] See http://www.comcast.net/terms/use/ .

[35] See http://networkmanagement.comcast.net.

[36] See http://www.comcast.net/privacy/ .

[37] See http://security.comcast.net/?cid=NET_33_0 .

disclosure statements to ascertain the extent to which these disclosure efforts constitute best practice.

It is also possible to overdo disclosure, to require a level of detail that might be fine for engineers with lots of time but is useless for regular customers and costly for ISPs to provide. In an extensive letter to the FCC,[38] Free Press states the importance of disclosure to enable customers to make intelligent decisions, and lauds Comcast's and AT&T's change of disclosure policies. But they go on to suggest that ISPs must disclose "the number of users on [each] shared Internet connection…total download and upload capacity of the shared network connection…peak utilization of each link in the network during periods of congestion…." and so forth. Given that broadband ISPs will have many thousands of shared connections, the request would produce mountains of operational and engineering data of no use whatsoever to regular customers. The key to determining what data should be disclosed is simple: what do *customers* want to know? And the key to finding this out is to ask real customers, not pundits and advocates.

Google is often lauded as an exemplar of openness, so an examination of Google's disclosure statements is informative. Their disclosure statements are accessible at the bottom of Google's homepage via the Privacy link. A comparison of the Comcast and Google disclosure statements shows that they are remarkably similar. The obvious differences are (i) Google's statements use less formal language and employ short YouTube videos; (ii) since Google offers many products, there is a privacy statement for each product; and (iii) Comcast devotes a web page to network management issues, while Google does not. But overall, they disclose about the same level of detail. Of course the reader is also invited to assess Google's disclosure statement using the principles and questions above.

One industry that has received much attention recently for its opaque disclosure policies is the credit card business. While a credit card disclosure chart has been mandated since 2000, it appears to be designed to confuse rather than inform. An interesting proposal suggests that credit cards carry the equivalent of a Nutrition Label and the authors actually design and display such a label, comparing it with the existing chart and with the Nutrition Label.[39] Even a complex product such as consumer credit can yield a disclosure solution which is easy to access, clear and simple. Perhaps this

[38] See Notice of *Ex Parte* filing, WC Docket 07-52, LETTER TO THE FCC from Ben Scott, *Free Press*, Oct. 24, 2008.

[39] See Gibson, D., Hall, C. and Harris, S., HEALTHY CREDIT, *New York Times* Opinion, May 23, 2009 at http://www.nytimes.com/2009/05/24/opinion/24gibson.html?_r=2 .

degree of accessibility, clarity and simplicity should be an objective for the broadband ISP industry.

The Australian Competition and Consumer Commission (ACCC) has taken a unique approach to disclosure of broadband speeds achievable by customers. This is a matter likely to be of substantial importance to customers but it is not covered at all by US broadband ISPs in current disclosures. The standard format for advertising broadband speeds is to quote maximum speeds, "up to 12 Mbps", without stating the conditions under which such speeds are actually attainable (if at all) by real customers (and without verification). The ACCC has issued very clear guidelines[40] to broadband ISPs concerning how they can advertise the speed performance of their service without running afoul of the Australian Trade Practices Act of 1974. The ACCC takes the position that accurate disclosure requires that speed test results actually achievable by real customers can be advertised, and variations occurring in the real world that affect customers must be prominently displayed in advertising. The ACCC does not at this time require verification of test results, although it is likely that falsification of test results in public statements could have significant consequences for the offending ISP.

Ofcom, the British telecommunications regulator, has adopted a rather aggressive disclosure policy. For several years, Ofcom has conducted wide-ranging broadband testing over a broad sample of British broadband households and reported the results publicly.[41] Additionally, Ofcom has encouraged broadband ISPs to adopt a voluntary Broadband Speeds Guide, with both a code for ISPs and a guide for consumers as to what speed and performance to expect from their ISP.[42] To develop these results, Ofcom has partnered with SamKnows, a British broadband firm that in 2008 developed the benchmark tests Ofcom uses.[43]

Another possibility is that customers can collectively provide performance measurements, using speed measuring websites, and using "wiki" approaches to organize the effort on the web, attempt to map out performance measures for different

---

[40] BROADBAND INTERNET SPEED CLAIMS AND THE TRADE PRACTICES ACT 1974, *ACCC Information Paper*, January, 2007, at http://www.accc.gov.au/content/index.phtml/itemId/779405 .

[41] The most recent test results are reported in CONSUMERS' EXPERIENCE OF FIXED-LINE BROADBAND, *Ofcom*, accessible at http://www.ofcom.org.uk/media/features/broadbandspeedsjy. A fuller report that discusses the testing methods and results is UK Broadband Speeds 2008, *Ofcom*, Jan 8, 2009, http://www.ofcom.org.uk/research/telecoms/reports/bbspeed_jan09/bbspeed_jan09.pdf . Note that the regulator is collecting and disseminating information, not the broadband ISP. Ofcom has taken on the disclosure role.

[42] See BROADBAND SPEED CODE, *Ofcom*, at http://www.ofcom.org.uk/media/features/broadcodejy .

[43] These benchmark tests are described at http://www.samknows.com/broadband/performance.php?page=performance-ofcom-and-samknows .

ISPs and different neighborhoods. Of course, this option is available to anyone now and no such "ISP performance wiki" has developed thus far. Should one develop, it is not clear how useful this would be, as measuring performance is an exacting engineering exercise and amateur efforts are likely to fall short of professional standards.

This brief and incomplete survey suggests that existing transparency/disclosure practices in the broadband ISP industry are a work in progress. Privacy disclosure (applicable to both broadband ISPs and application providers) is the subset of disclosure issues which has the longest history and the benefit of long-term FTC scrutiny. The regime of self-regulation apparently has produced uneven results. Disclosure of other material facts has only recently emerged, beginning from a very low base. Again, self-regulation is the regime in place. Whether this is sufficient to ensure the four principles for disclosure stated earlier is a matter for policymakers to decide.

Disclosure Challenges in the Broadband ISP Industry

It is one thing to enunciate principles of disclosure that represent an ideal, it is quite another to implement them in the context of broadband ISPs. This industry represents special challenges, which even with the best of intentions make realizing the disclosure principles difficult. I mention a few of the obvious challenges, and suggest avenues to be explored for solutions.[44]

1. If speed performance of a broadband ISP is to be disclosed, exactly what speed is it that's disclosable? The problem is that maximum speeds are likely irrelevant to most customers who will never realize such speeds. Thus, actual speeds vary moment by moment as traffic ebbs and flows on the network, and other customers come and go. It also depends upon traffic in the wider network, beyond the ISPs immediate distribution system, as well as limitations of the customer's gateway, firewall or personal computer. There is no single speed that any customer is guaranteed, so what is to be disclosed?
    - The ACCC report suggests a direction. Test results can determine based on historical usage patterns both average upload and download speeds as well as variation in speeds. These speeds may depend upon the level of service chosen by the customer, and the variability may depend upon factors such as loop length for DSL. A parsimonious presentation of such results would be both useful and accurate, providing customers with

[44] I explicitly disclaim any expertise in software, web design, information presentation, or consumer psychology. I offer suggestions simply to illustrate that challenges may be met and progress is possible.

information relevant to purchase decisions.

Developing a standardized test and standardized presentation format would greatly improve the effectiveness of disclosure. Ofcom's benchmark tests using SamKnows technology appears to be a very promising direction, and demonstrates that this complex problem can be solved. However, several issues must be kept in mind:

- End-to-end customer performance depends not only on broadband ISP performance but on customer configuration (LAN, router, etc.) and backbone performance as well as well as destination ISP performance. A test of a broadband ISP's speed should be just that, and not depend on other links in the Internet chain.
- Broadband performance not only depends on network congestion (and time of day, etc.) but on system configurations, such as length of loop (for DSL) and number of households on a hub or node (for cable). Measuring average speed (and variance) can be misleading if neighborhood configurations are not factored in.

A simple example is the EPA requirement for disclosure of vehicle fuel efficiency for new automobiles. A sticker is required listing both city and highway miles per gallon in standard format. It is generally recognized that these miles per gallon are rather optimistic and not reflective of the mileage a particular drive will achieve, but they do form a good basis for comparisons among vehicles.

2. "Easy access" makes much more sense for a packaged good, in which disclosure is right on the label, than for a digital service such as broadband ISP for which the customer does not actually see any tangible evidence of the service while using it. Even for a website, the best that can be done is to provide links to "terms of use" web pages.
    - The usual practice with websites today is to present these links rather inconspicuously on the opening page in the smallest type. An alternative would be to use a standard icon in the upper right-hand corner of the opening webpage;[45] rolling the mouse pointer over the icon would cause a dropdown menu to appear, listing Help, Terms and Conditions, Personal Information or Privacy as options that would take the user to the relevant

[45] Example icon: 

page.

For a broadband ISP, the problem is more difficult, as there is literally no "package" on which to place the label. One option would be that when the customer is connected to the broadband ISP, an icon would appear in the customer's SysTray (for Windows users) which would function in the same way as the as the website icon described above. This icon could be proprietary (to avoid confusion with the standard website icon above). Of course, the customer would have to opt-in (or opt-out) of having this functionality.

3. Broadband is a complex service with lots of parameters; keeping things simple and clear is difficult when the ISP is presenting a terms and conditions contract, or network management policy.
   - The model here would be prescription medications, which are every bit as complex as broadband. Disclosure is two-level; the first level is the most important (to the customer) disclosures in brief with easy access (package label). The second level is more complete, more detailed and more like a terms and conditions contract (package insert).

     The Google privacy policy disclosure provides an interesting avenue; basic information is described in simple, short videos, understandable by people without an advanced degree in law or engineering.[46] More complete and detailed information is linked to from the basic information. In this regard, application providers and ISPs have an advantage over the FDA and the pharmaceutical industry in that short, simple videos are an available disclosure mechanism. Additionally, ISPs and application providers can use the by-now standard of Frequently Asked Questions (FAQs) which can provide detailed information in a format comprehensible to regular people.
4. Broadband ISPs have a wide range of business relationships with application providers, other ISPs and other network providers. Does this complex web of relationships need to be disclosed to customers?
   - Only to the extent that these business relationships affect a reasonable customers' purchase decisions. For example, it is probably important to disclose if an ISP is blocking certain websites or other data streams (say, kiddie porn and worms/viruses). By way of example, the clear and

[46] AT&T's on line privacy policy also makes effective use of videos.

simple disclosure might include the principles the ISP uses to block; the more detailed disclosure might include why they are blocked.

Some ISPs may have preferential relations with application providers, affording them caching services, Quality of Service-based traffic handling, etc. Should these relationships necessarily be disclosed? Again, only insofar as it affects a reasonable customer's purchase decisions. This is a gray area which is likely best handled on a case by case basis.

5. Malware is a growing threat to the Internet, which hurts both customers and ISPs. Customers expect ISPs to vigorously defend them, but what are the disclosure implications of this emerging problem?
   - This presents interesting disclosure tradeoffs. It is likely that customers will look to their ISPs for protection from these threats, but will be unhappy if site blocking is excessive. Should we require that each site blacklisted as a suspected spam source be identified and listed? As a security issue, this is probably a bad idea because it lets the bad guys know what the ISP's blacklist policy is and affords them the intelligence to effectively work around the ISP's defenses.

     This also highlights the role of the customer in protecting not only their own computers and broadband connection, but those of other customers on the ISP's network. No one wins when hackers turn machines into zombies, and customers bear some responsibility for safe computing. Broadband ISPs may have a responsibility to disclose malware dangers (for example, downloading software which is impossible to fully uninstall, leaving bits of malware on a customer's computer), and perhaps offer to provide software that detects, notifies and eliminates malware on customers' computers.

In summary, the nature of the broadband business leads to unique problems and challenges in achieving model disclosure. This section suggests that these problems are not insurmountable, and disclosure need not be an onerous task for the industry. Even if mandatory disclosure is not adopted by policymakers, ISPs need to be aware that as this industry matures, its customers will expect more of them and full and clear disclosure may become a competitive necessity for their business.

Conclusion

The purpose of this paper is *not* to determine what broadband ISPs should be required to disclose. The purpose of this paper is threefold:

1. To provide a framework for analysis of appropriate disclosure. I formulate four principles: (i) disclose facts *relevant for customers' purchase decisions*; (ii) ensure *access* to disclosed information *is easy*; (iii) disclosure information must be *clear and simple*; and (iv) disclosed information must be *verifiable*. These principles are supported by reference to successful models of disclosure elsewhere in the economy.
2. To provide a comparative review (unfortunately brief and incomplete) of (i) existing practices in the broadband industry and how these practices are evolving; (ii) existing practices associated with privacy policies (for both broadband ISPs and application providers) and the FTC's involvement in these practices; and (iii) disclosure practices in other countries, to the extent information is available.
3. To provide a brief review of some of the challenges for disclosure inherent in the broadband ISP industry, with suggestions about how these difficulties might be overcome.

There are, of course, a host of issues concerning this industry of policy importance, such as network neutrality, investment issues, rural deployment, pricing, network management, and competition, among many others. This paper is tightly focused only on the transparency/disclosure issue, leaving these broader issues to other work. I find that disclosure is likely an important issue for customers of broadband ISPs, and the response of these firms for disclosure is evolving rather rapidly. Whether policy intervention is needed at this point depends upon factors beyond this paper.